Scalable Network Security for the Virtualized Data Center
Table of Contents

As Data Centers Evolve, So Do Security Needs 3
  Physical to virtual infrastructure 3
  Virtualized applications to private clouds 3
  Multitiered to flat network architectures 4
  The rise of advanced persistent threats 4
The Stakes Are High 4
A New Security Model for the Virtualized Data Center 5
Step Up to McAfee Network Security Platform 8
As Data Centers Evolve, So Do Security Needs

Today’s enterprise data centers are undergoing a period of intense evolution. Virtualization and cloud computing are changing the way IT organizations deliver services, creating new opportunities to reduce costs, increase efficiencies, and accelerate business operations. These innovations are transforming the data center, replacing physical infrastructure with flexible pools of virtual assets that can be scaled and re-configured dynamically.

In a recent Network World survey, 62 percent of respondents planned to virtualize at least 40 percent of their servers by year end, with one-third targeting 60 percent. Fully half had already implemented a private cloud within their infrastructure or planned to do so within the next three years.

But as organizations make the transition from application-specific virtualization to full-scale dynamic clouds, many are discovering that application security can break down when subjected to data center-wide server virtualization and application mobility. Equally problematic is the fact that most conventional security solutions can’t meet the performance requirements of the flat, high-capacity network fabrics required for cloud-scale virtualization. Securing a cloud environment demands new best practices and a security model fully adapted to the challenges of four critical transitions taking place within our data centers and in the threat environments that surround them.

Physical to virtual infrastructure

In a conventional data center with applications running on dedicated physical servers and connected by networks of physical cables and switches, the hardware affords an element of isolation, a natural framework for defensible trust boundaries. When that physical infrastructure is virtualized, new strategies are required to create and maintain those boundaries in the absence of physical partitions. Another problem is the inter-machine communication that moves into the virtual environment along with the virtual machines—beyond the reach of physical security controls.

Virtualized applications to private clouds

The transition to a true cloud platform brings an unprecedented level of dynamism into the data center environment. Virtual machines are continuously launched, moved, and decommissioned as workloads change around the clock. Correctly applying security policy and detecting threats in real time requires the ability to accurately track applications, recognize users, correlate events, and analyze behaviors in a constantly changing environment. Without it, blind spots that are unmanaged and insecure develop quickly.
Multitiered to flat network architectures
Cloud environments experience frequent large-scale data transfers as the virtual infrastructure is reconfigured to accommodate changing workloads. They also generate large volumes of east-west traffic between virtual machines and storage. Multitiered architectures adopted from the enterprise network are proving too slow and inflexible and are giving way to flatter, non-blocking 10 GbE fabrics with the ability to connect tens of thousands of nodes.

The rise of advanced persistent threats
Attack strategies continue to gain sophistication, the most insidious example being the emergence of advanced persistent threats (APTs)—targeted attacks designed for stealthy penetration, long-term surveillance, and large-scale data theft. Many APTs have shown the ability to migrate through an environment, compromising system after system without creating the telltale traffic that typically signals malware propagation.

The Stakes Are High
The business impacts of a large-scale data breach can be widespread and long-lasting. Services can be interrupted for investigation and remediation. Victims of personal data loss must be notified and compensated. Often there are regulatory fines, class action lawsuits, and public relations costs. The damage to brand and business and customer relationships can be devastating. Consider a few examples from 2011 alone:

• Sony Corporation has experienced more than a dozen separate breaches, mostly occurring during 2011, affecting Sony PlayStation Network, Sony Online Entertainment, Sony Pictures, and other company sites. More than 77 million customer records were compromised overall, with total cost estimates ranging upwards from $171 million.

• Epsilon, the world’s largest permission-based email marketing provider, suffered a massive breach in April. The company sends more than 40 billion emails annually for more than 2,500 clients, including seven of the Fortune 10. More than 60 million customer email addresses were compromised, for clients that included Kroger, US Bank, JPMorgan Chase, Capital One, and Home Shopping Network, among many others.

• RSA, the security division of EMC Corporation, endured one of the most humbling breaches of 2011. Attackers stole proprietary information relating to the company’s SecureID product, one of the world’s most widely used two-factor authentication solutions.
A New Security Model for the Virtualized Data Center

Organizations that are preparing their data centers for full-scale virtualization need a new approach to security that fully supports the unique operational challenges of a cloud environment. Key considerations include:

• **Scalable performance**—Security controls must match the throughput of today’s flat, high-capacity data center networks without introducing latency. Like the networks themselves, the security platforms must scale out incrementally and affordably to accommodate growth over time.

• **The flexibility to adapt to virtual environments**—Security controls for virtual environments can’t be limited to scanning the traffic entering and leaving physical servers. They must have direct access to all the traffic within the virtual network itself—between virtual machines, storage, and the hardware layer.

• **The ability to recognize users and applications**—When physical landmarks are abstracted by virtualization, security controls must be able to identify systems, applications, and users to track them as they move through the virtual environment, and to accurately apply the appropriate policy.

• **An extensible security model capable of stopping advanced attacks**—In the virtual environment, as in the physical one, signature-based inspection is no longer adequate to detect and stop targeted attacks and advanced persistent threats. Multifactor inspection is essential, coupled with context awareness, behavioral analytics, and external reputation intelligence to identify unknown and zero-day threats.

• **Streamlined integration**—The same security controls should be used to defend both the physical and virtual environments. All the controls in use should be manageable through a single management console.


Today, only one network security solution delivers on the essential requirements of network security in the virtual data center. Only McAfee® Network Security Platform combines advanced threat detection, scalable in-line performance, and next-generation network intrusion prevention system (IPS) controls that operate seamlessly across physical and virtual environments.

• **Unflinching performance for modern data center network fabrics**—McAfee Network Security Platform features a highly efficient inspection engine and native 10 GbE connectivity. It’s capable of maintaining line rate performance in flat, high-capacity network fabrics, even with aggressive security policies and variable, real-world traffic conditions that reduce throughput in many alternative solutions by up to 50 percent.

• **New scalable solution pushes IPS performance to 80 Gbps**—The new McAfee Network Security Platform XC Cluster allows McAfee Network Security Platform to scale gracefully up to 80 Gbps of throughput and 40 million concurrent connections, effectively doubling existing ISP benchmarks. Now your IPS solution can scale as your virtual environment grows, eliminating expensive rip and replace upgrades. Load balancing and failover capabilities support optimum efficiency and high availability.
**Integrated inspection for physical and virtual environments**—McAfee Network Security Platform includes native inspection of virtual environments through full integration with the VMware vShield API. Now you can inspect traffic and enforce policy on and between virtual machines, regardless of their physical residence. Native access to VCenter tools lets you integrate network security across virtual environments.

**Identity-aware security**—McAfee Network Security Platform features identity-aware policy enforcement that enables accurate, automatic, and consistent application of policy across physical, virtual, and cloud environments. Security profiles move dynamically with their virtual machines, and McAfee Network Security Platform tracks the physical host residence of every virtual machine.

**Multifactor traffic inspection to spot and stop advanced threats**—McAfee Network Security Platform features an ultra-efficient inspection architecture that fully characterizes attacks based on a comprehensive and extensible range of detection methods, including:

- Signature-based and statistical anomaly detection with stateful inspection and vulnerability-based signatures
- Protocol anomaly detection that identifies deviations from normal usage based on behavior and state
- Heuristic analysis that is particularly effective in identifying bot infections and SQL injection attacks
- Continuous, real-world threat research from McAfee Global Threat Intelligence™ file and IP reputation technology with always-on protection that uses signature and behavioral-based scanning to reduce exposure from unknown threats. McAfee Global Threat Intelligence file and IP reputation quarantines and blocks threats in real time and closes any protection gap in your security.
• **Application awareness**—McAfee Network Security Platform provides layer 7 detection and identification of more than 1,100 applications, including granular visibility into sub-applications, like the growing Zynga portfolio of Facebook games, and IRC chat in Yahoo! Mail. For each application McAfee Network Security Platform provides analytics and graphical reporting for essential metrics, including risk rating, aggregate threats, and bandwidth consumed. Enhanced rule definition simplifies application access control and includes the ability to correlate application activity with network attacks to enable more intelligent response and enforcement decision-making.

• **Integrated security management**—McAfee Network Security Platform, when integrated with McAfee® ePolicy Orchestrator (McAfee ePO™) software, enables a consolidated view of risk and compliance across the enterprise, including up-to-the-minute assessments of at-risk infrastructure based on system vulnerabilities, network defenses, and endpoint security levels.

• **Multitenancy features for telecommunications and service providers**—McAfee Network Security Platform includes granular multitenancy options that are purpose-built for service provider environments. Create up to 1,000 virtual IPS policies per appliance, with granular policy control and unique rule sets in each. The solution also includes features for mobile service providers, allowing management of network policies for separate customers or services.

Figure 3. McAfee Network Security Platform allows users to create up to 1,000 virtual IPS policies, each with granular controls and reporting, making it ideal for service provider environments.
Step Up to McAfee Network Security Platform
The transformation of enterprise data centers by large-scale virtualization and private cloud developments demands an equally innovative approach to network security, one that combines a comprehensive threat detection model with extremely high levels of inspection efficiency, scalable performance, native integration with key virtualization technologies, and single-console management integration. That solution is now available, from McAfee. To learn more about McAfee network solutions for the data center, visit www.mcafee.com/datacenter_networks.

About McAfee
McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world’s largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com.

3 Information Week, “6 Worst Data Breaches Of 2011,” op. cit.